ThreatConnect and Zscaler

Enabling joint users to proactively protect their organizations by integrating ThreatConnect's TI Ops Platform and Zscaler Internet Access (ZIA)

The Challenge

Digital enterprises rely on ubiquitous network connectivity across the globe, leading to access and exposures ripe for abuse by threat actors. They successfully leverage pervasive network access to compromise end-user devices and enterprise systems, leading to ransomware attacks and data breaches.

Why ThreatConnect + Zscaler

Zscaler Internet Access (ZIA) is a security platform, delivered from the cloud, that sits between users and the Internet. ZIA secures users by providing full protection from online threats. Zscaler allows organizations to easily scale protection to all offices and users, regardless of their location.

With ThreatConnect's TI Ops Platform, users gain relevant, actionable, and high-fidelity insights from a single source of threat intelligence "truth". Leveraging the ThreatConnect Threat Library, users can take action by delivering high-fidelity threat intel to ZIA, amplifying its threat detection and prevention capabilities, and making organizations more resilient to attacks.

Key Benefits

- Flexible and granular control over which indicators are sent to ZIA to monitor and block threats.
- Use ThreatConnect Playbooks to automatically alert or block/unblock connectivity in ZIA based on an indicator's threat rating
- Retrieve full reports from Zscaler Sandbox to add context to the threats tracked in the ThreatConnect Platform

ThreatConnect.
ThreatConnect.com
3865 Wilson Blvd., Suite 550
Arlington, VA 22203

sales@threatconnect.com
1.800.965.2708

Get Results with ThreatConnect + Zscaler

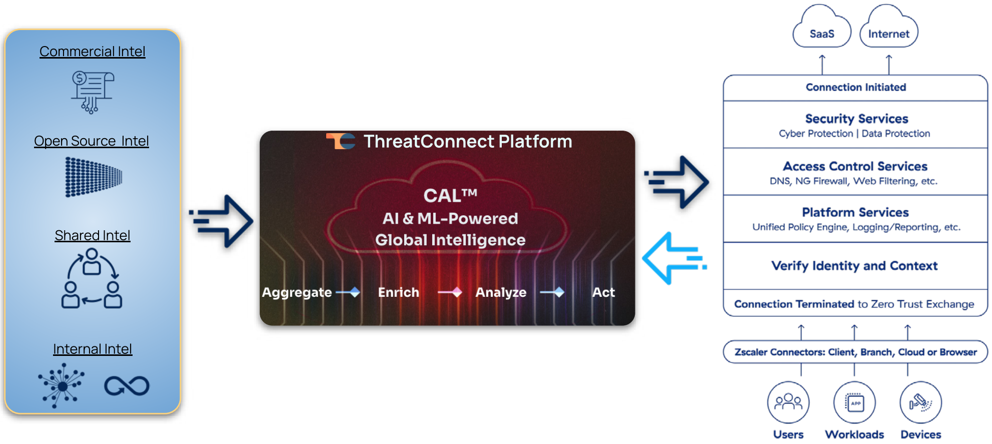
The ThreatConnect ZIA Playbook and Job Apps make integrating the ThreatConnect Platform and Zscaler ZIA fast and easy. These support DLP Dictionaries, Allowed and Blocked URLs, and the Sandbox, and enable use cases like:

Smarter Threat Detection and Prevention

Proactively block threats in Zscaler with the power of the ThreatConnect Platform. Users can send high-precision indicators of compromise to the Zscaler Denylist for automated blocking or alerting leveraging ThreatConnect's ThreatAssess score. ThreatAssess is an in-platform scoring system that captures the criticality of an Indicatorto help prioritize threats.

Threat Hunting

When integrating Zscaler and ThreatConnect, users can automatically retrieve Sandbox results from Zscaler, correlate the results with known intelligence sources in the ThreatConnect Threat Library, and use integrations with other security tools to extend threat prevention and blocking to endpoints and the cloud. Analysts can create repeatable, automated "threat hunts" on findings from the ZIA Sandbox leveraging Automation and Playbooks in the ThreatConnect Platform.



How to Get Started

ThreatConnect customers that want to learn more about Zscaler ZIA, please visit https://www.zscaler.com/products/zscaler-internet-access. Already have Zscaler ZIA? Visit the App Catalog in the ThreatConnect Platform to implement the Zscaler App or reach out to Customer Success for assistance.

ThreatConnect.

ThreatConnect enables threat intelligence operations, security operations, and cyber risk management teams to work together for more effective, efficient, and collaborative cyber defense and protection. With ThreatConnect, organizations infuse ML and AI-powered threat intel and cyber risk quantification into their work, allowing them to orchestrate and automate processes to get the necessary insights and respond faster and more confidently than ever before. Over 200 enterprises and thousands of security professionals rely on ThreatConnect every day to protect their organizations' most critical assets.

www.threatconnect.com

+1-703-229-4240

sales@threatconnect.com

zscaler™

Zscaler (NASDAQ: ZS) accelerates digital transformation so customers can be more agile, efficient, resilient, and secure. The Zscaler Zero Trust Exchange™ platform protects thousands of customers from cyberattacks and data loss by securely connecting users, devices, and applications in any location. Distributed across more than 150 data centers globally, the SSE-based Zero Trust Exchange™ is the world's largest in-line cloud security platform.

www.zscaler.com/company/contact

+1-408-533-0288